DELL Technologies

零時差：透過 Dell Technologies 強化網路安全和復原能力

零時差攻擊威脅不斷升高

在現今網路安全性態勢中，零時差攻擊已迅速升級為最艱鉅的挑戰之一。這些攻擊利用軟體供應商和安全性專家未知的漏洞，使企業毫無準備並暴露在風險下。從醫療保健到金融，各行各業的組織都容易受到此類缺口的影響，這通常會造成嚴重的財務和營運後果。

數位轉型的步伐正在加快，而零時差攻擊也變得更加頻繁和複雜。對強大保護措施的需求從未如此迫切。Dell Technologies 瞭解此威脅的關鍵性質，並為企業提供創新且可擴充的防禦機制，以有效抵禦零時差攻擊並從中復原。

什麼是零時差攻擊？

零時差攻擊是指在有可用的修補程式或修正之前，利用軟體或硬體中未公開的安全性漏洞。攻擊者會利用這段有機會的時間，因此通常會在漏洞被發現和解決之前，造成大範圍的中斷。

零時差攻擊的運作原理

1. **探索漏洞：**駭客會找出軟體應用程式或系統中的編碼瑕疵，或隱藏的後門。
2. **開發利用漏洞的方式：**建立惡意軟體以利用該漏洞。攻擊者可能會使用有針對性的網路釣魚活動，或充滿惡意軟體的網站，來利用漏洞。
3. **執行攻擊：**部署利用漏洞的方式，入侵系統，並可能造成資料竊盜或作業干擾。

常用技巧

- 路過式下載會誘使使用者在不知情的情況下，安裝惡意軟體。
- 網路釣魚電子郵件會散佈惡意連結或酬載，以利用漏洞。
- 無檔案式攻擊透過完全在系統記憶體中執行作業，來逃避偵測。

這些極其先進的攻擊媒介，讓零時差攻擊變得特別危險，因為傳統的簽章型偵測工具通常無法識別它們。

© 2025 Dell Inc. 或其子公司。

對企業的影響

零時差攻擊因其不可預測性和偵測延遲，而帶來重大風險。可能會在幾個方面造成災難性的後果。

財務損失

成功的零時差攻擊可能會導致巨額成本，包括從監管機關罰款，到停機期間的收入損失。例如，在電子商務平台中，遭到利用的不明漏洞可能會停用結帳流程，進而直接影響銷售。

聲譽影響

大眾對公司的觀感可能會受到不可挽回的損害。當敏感資訊暴露或服務失敗時，客戶會對公司失去信任。

營運中斷

未解決的漏洞通常會癱瘓系統，導致生產力下降、專案延遲和錯失商機。

真實的例子

一家大型醫療保健供應商淪為零時差攻擊的受害者，該攻擊鎖定未修補的醫療裝置軟體。這次攻擊中斷了關鍵作業，曝光患者資料，並使組織損失**數百萬**的復原費用，同時也讓患者信任崩塌。

令人震驚的統計資料

2023 年 Ponemon 的一項研究指出，涉及零時差的漏洞百分比約為 80%

零時差攻擊持續呈現超過

70% 遭到利用的漏洞

資料來源：2024 年：Mandiant《M-Trends》

透過 Dell Technologies 對抗零時差攻擊

Dell Technologies 提供領先業界的解決方案，協助企業主動防範零時差攻擊，同時在此類攻擊發生後促進快速復原。

伺服器和儲存安全性解決方案

Dell 的伺服器和儲存安全性解決方案可提供額外的保護層：

- 安全伺服器會監控並封鎖未經授權的存取嘗試。
- 資料備份與復原系統確保即使在最壞的情況下，關鍵資訊也能保持可存取和完整。

採用 Dell Trusted Device 的強化端點

端點是攻擊者的關鍵進入點。Dell Trusted Device 內嵌進階安全性措施，確保端點免受未發現的威脅影響。

- **SafeBIOS** 可保護韌體免於遭到操縱，徹底確保系統完整性。
- **SafeID** 透過保護驗證程序，來保護使用者憑證。
- **SafeData** 對靜態和傳輸中的敏感資料進行加密，使其在遭攔截或利用時毫無用處。

© 2025 Dell Inc. 或其子公司。

透過 CrowdStrike 主動偵測威脅

CrowdStrike 運用進階分析和 AI，監控端點活動，偵測表示可能有零時差利用的異常行為。其主動式威脅偵測功能，可確保在漏洞造成廣泛損害之前，快速回應。

舉例來說，一家使用 CrowdStrike 的電信供應商，由於可及早偵測網路流量的異常狀況，因此緩解了客戶伺服器上潛在的零時差利用。

Dell PowerProtect 解決方案

Dell PowerProtect 提供強大、不變的備份與隔離復原選項。在零時差攻擊之後，企業可以快速有效地恢復營運，維持業務連續性並保護重要客戶資料。

舉例來說，有家大型連鎖零售商店使用 PowerProtect，在因零時差漏洞造成勒索軟體攻擊，使得檔案遭入侵時，用來復原加密檔案，避免長時間停機。

使用 Dell PowerSwitch 網路與 SmartFabric OS 的進階網路安全性和微區段

透過在整個基礎架構中，提供進階網路切分、嚴格的存取控制和即時流量分析，增強對零時差攻擊的防禦。

多層式安全防護方法的重要性

真正的安全性需要不止一種解決方案。多層式策略結合了技術、程序及人員，構成全方位的保護架構。

加強防禦的關鍵行動

- **採用零信任原則：**驗證嘗試存取網路的每個人和裝置。
- **實施進階加密：**使用加密通訊協定，保護傳輸中資料及靜態資料。
- **教育員工：**提供詳細的訓練課程，教員工如何識別網路釣魚嘗試和社交工程手法。
- **定期測試系統：**執行一致的滲透測試和漏洞掃描，以確保防禦措施能夠適應新威脅。

Dell Technologies 將這些實務與其進階安全性解決方案搭配，確保組織已準備好有效對抗零時差漏洞。

加強網路安全的夥伴關係

Dell 與業界領導者 **Microsoft**、**CrowdStrike** 及 **Secureworks** 合作，為客戶提供尖端的安全性情報和工具。

- **Microsoft** 與 Dell 解決方案順暢整合，以確保全系統的相容性和主動式保護機制
- **CrowdStrike** 提供進階端點威脅情報，以偵測潛在的零時差利用。
- **Secureworks** 可提供持續監控和專家補救措施，用於即時攻擊回應。

運用 Dell Professional Services

Dell Professional Services 提供全方位的諮詢、實作及復原協助，有助於企業解決和減輕零時差威脅帶來的相關風險。從事件回應到網路安全藍圖規劃，Dell 可協助組織實現長期復原能力。

© 2025 Dell Inc. 或其子公司。

打造具韌性的未來

投資 Dell Technologies 代表擁有不僅能提供卓越技術，還能讓您完全安心的合作夥伴。透過尖端解決方案、策略合作關係及無與倫比的專業知識，Dell 讓組織能夠預測和偵測最先進的零時差攻擊，並從中復原。

請立即聯絡 Dell Technologies，以保障您的業務、保護您的聲譽，並在無法預測的數位環境中蓬勃發展。相信 Dell 能強化您的未來，抵禦日後的威脅。

Dell Technologies 透過專門保護重要事物的安全性解決方案和服務，激發企業信心，協助企業在不斷演進的零時差攻擊挑戰中領先一步。

造訪 **Dell.com/SecuritySolutions**，瞭解如何解決現今一些主要的網路安全挑戰

深入瞭解
Dell 解決方案

聯絡 Dell
Technologies 專家

檢視更多資源

使用
#HashTag 加入對話

© 2025 Dell Inc. 或其子公司。保留所有權利。Dell 與其他商標均為 Dell Inc. 或其子公司的商標，其他商標是其各自擁有者之商標。

DELL Technologies